5
Vragenuur: Vragen Ten Broeke

Vragen van het lid Ten Broeke aan de minister van Defensie over **het bericht dat de U.S. Central Command is gehackt door ISIS(-sympathisanten)**.

☐

De heer **Ten Broeke** (VVD):
Zo is het, voorzitter. Het is goed dat u deze vraag hebt toegestaan.

Voorzitter. Gisteren werden de accounts van het U.S. Central Command op Twitter en YouTube gehackt. De groep die de hack uitvoerde, noemde zich het Kalifaat en beweert ISIS te steunen. Het U.S. Central Command voert vanuit Tampa, Florida het bevel over alle Amerikaanse militairen in het Midden-Oosten, Noord-Afrika en Centraal-Azië. Dit is het zenuwcentrum van Amerikaanse militaire operaties in maar liefst twintig landen, waaronder Afghanistan en Irak. Dit zenuwcentrum coördineert ook de internationale coalitie die ISIS bestrijdt in Irak en Syrië en daarmee dus ook de Nederlandse bijdrage. Een bericht op de twitter feed van het Central Command luidde: American soldiers, we are coming, watch your back. Was getekend, ISIS.

Dit alles moet alarmbellen doen afgaan, niet alleen in Washington maar ook hier bij ons. De hack vond plaats precies op het moment dat president Barack Obama een toespraak hield over internetveiligheid en daarbij onder andere inging op een andere hack die veel opzien baarde, namelijk die van Sony Pictures door waarschijnlijk Noord-Korea. Uiteraard is er een groot verschil tussen data-inbreuk en het hacken van een twitteraccount en tussen commerciële informatie en defensie-informatie en -infrastructuur, maar elke inbreuk op de veiligheid, zeker op dit niveau, roept de vraag op of we voldoende weerbaar zijn tegen cyberaanvallen.

Ik heb vier vragen. Hoe kon dit gebeuren? Is er vertrouwelijke informatie verkregen bij deze hack? Zijn daarbij veiligheidsbelangen, ook Nederlandse veiligheidsbelangen, in het geding geweest? Het U.S. Central Command geeft in een persbericht aan dat er geen operationele impact is geweest. Kan de minister dat bevestigen? Wie onderzoekt dit eigenlijk? Doet het U.S. Central Command dat zelf, of doet de FBI dat? Worden de uitkomsten van het onderzoek met ons gedeeld? Het U.S. Central Command geeft in een persbericht ook aan dat het deze hack louter ziet als een geval van cybervandalisme. Deelt de minister die opvatting, of ziet zij toch aanleiding om wat serieuzere vragen aan de Amerikanen te stellen over fundamentele kwetsbaarheden bij cyberaanvallen?

Ten slotte verschenen er op de Twitterpagina van Central Command ook persoonlijke gegevens van militairen, onder wie hoge officieren. Het zou gaan om adresgegevens, e-mailadressen en telefoonnummers. Was deze informatie al openbaar? Zitten er Nederlandse militairen bij?

☐

Minister **Hennis-Plasschaert**:
Voorzitter. Dat zijn een heleboel vragen. CENTCOM heeft gisteren inderdaad bevestigd dat de Twitter- en YouTube-accounts voor ongeveer 30 minuten zijn gecompromitteerd. Het incident wordt op dit moment onderzocht. De heer Ten Broeke vroeg mij of CENTCOM dat zelf doet of dat de FBI daarbij betrokken is. Ik weet niet welke diensten erbij betrokken zijn, maar feit is dat CENTCOM het onderzoek in gang heeft gezet en dat verschillende diensten daar vanuit hun expertise bij zullen worden betrokken. Er is te kennen gegeven dat de uitkomsten van het onderzoek, als zij daartoe aanleiding geven, met Nederland zullen worden gedeeld. Laat ik wel helder zijn: het hacken van Twitter- of YouTube-accounts is niet heel erg ingewikkeld: het kan u en mij ook overkomen. Deze sites draaien op de zogenoemde commerciële servers. CENTCOM heeft daarover gisteravond zelf ook het nodige gezegd. Het is inmiddels duidelijk dat de door CENTCOM aangestuurde operaties niet zijn gecompromitteerd. De veiligheidsbelangen van de coalitie zijn dus niet in het geding geweest. Ook de Nederlandse veiligheidsbelangen zijn dus niet in het geding geweest.

CENTCOM zelf spreekt over een geval van cybervandalisme. Er is gevraagd of ik die mening deel. Ik heb in ieder geval geen aanleiding om daaraan te twijfelen.

Iets anders wat opviel — de heer Ten Broeke zei het zelf — is dat het getekend was door ISIS. IS zelf spreekt eigenlijk zelden of nooit over ISIS maar altijd over IS. Het kan dus goed zijn dat het een actie is van sympathisanten van IS. De informatie die is gelekt, lijkt niet geheim. Ik heb net verwezen naar het onderzoek; dat zullen wij even moeten afwachten. Het is inmiddels wel duidelijk dat veel documenten en afbeeldingen die gisteravond naar buiten zijn gekomen, eerder op openbare websites zijn gepubliceerd. CENTCOM heeft inmiddels ook aangegeven dat iedereen van wie persoonlijke informatie naar buiten is gekomen, door CENTCOM zal worden benaderd. Ik heb nu geen aanleiding om te veronderstellen dat er ook informatie bij zat van Nederlandse militairen, maar als dat wel zo is, zullen wij door CENTCOM worden benaderd. Nogmaals: ook de uitkomsten van het onderzoek zullen, als zij daartoe aanleiding geven, met Nederland worden gedeeld.

De heer **Ten Broeke** (VVD):
Ik denk dat het belangrijkste deel van het antwoord van de minister is dat de veiligheidsbelangen niet in het geding zijn geweest, noch die van de coalitiepartners, noch die van Nederland. Die verzekering moet worden verkregen, want de operaties zijn erg gevoelig en het niveau waarop de veiligheidsbelangen in het geding zouden kunnen zijn geweest, is erg hoog. De minister zei ook: het is een relatief eenvoudige operatie; het zou ook bij uw of mijn Twitteraccount hebben kunnen gebeuren. Ik dacht even dat ze ging zeggen dat wij het zelf hadden kunnen doen; dan slaat zij in ieder geval mij te hoog aan. We moeten er wel 100% zeker van zijn dat dit soort zaken — we hebben ook gezien wat er bij Sony is gebeurd — zich in de toekomst niet kan voordoen. Daarom stel ik een paar aanvullende vragen. Ziet de minister in deze gebeurtenis toch een aanleiding om nog eens heel scherp te kijken naar de Nederlandse krijgsmacht en zijn partners, die ook operaties coördineren? Zijn wij voldoende beschermd tegen cyberaanvallen? Heeft de Nederlandse krijgsmacht ook gevoelige of geclassificeerde informatie op commerciële servers staan? Kan de minister garanderen dat die informatie, die kennelijk eenvoudiger te hacken is, toch veilig is?

Minister **Hennis-Plasschaert**:
De heer Ten Broeke heeft natuurlijk helemaal gelijk als hij zegt dat echt de verzekering moet worden verkregen dat operatiegevoelige informatie niet is gecompromitteerd. De eerste aanwijzingen zijn dat dit niet zo is. Dat is bevestigd. Ik heb net al verwezen naar het onderzoek. Ook ik zal de uitkomsten daarvan moeten afwachten, maar ik heb vooralsnog geen aanleiding om te twijfelen aan de woorden die CENTCOM gisteren en vandaag duidelijk heeft uitgesproken.

Cybersecurity is een permanent onderwerp van aandacht. In zijn algemeenheid zeggen we dat garanties nooit voor de volle honderd procent kunnen worden gegeven. Het is niet alleen voor Nederland een permanent punt van aandacht, maar ook voor onze coalitiepartners, voor de NAVO en de Europese Unie.

Geclassificeerde informatie wordt bij Defensie nooit op commerciële servers gezet. Dat zijn ook de instructies die de medewerkers meekrijgen. We hebben in het verleden wel meegemaakt dat een medewerker spontaan iets naar zijn Gmail-account stuurde. Ook dan kom je in aanraking met een commerciële server, maar er wordt steeds op gestuurd en het wordt steeds in de gaten gehouden. Garanties zijn er niet in het leven, maar er wordt alles aan gedaan omdat cybersecurity de sleutel is voor bijna alle militaire operaties anno 2015.

De **voorzitter**:
Ik dank de minister voor haar antwoorden en voor haar komst naar de Kamer. Daarmee is er een einde gekomen aan het eerste mondelinge vragenuur van het nieuwe jaar.